information

Review

Blockchain and Machine Learning: A Critical Review on Security

Hamed Taherdoost [1,2,3]

[1] Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, BC V6B 1V9, Canada; hamed.taherdoost@gmail.com or hamed@hamta.org; Tel.: +1-236-889-5359
[2] Hamta Group, Research and Development Department, Hamta Business Corporation, Vancouver, BC V6E 1C9, Canada
[3] College of Technology and Engineering, Westcliff University, Irvine, CA 92614, USA

Abstract: Blockchain is the foundation of all cryptocurrencies, while machine learning (ML) is one of the most popular technologies with a wide range of possibilities. Blockchain may be improved and made more effective by using ML. Even though blockchain technology uses encryption to safeguard data, it is not completely reliable. Various elements, including the particular use case, the type of data, and legal constraints can determine whether it is suitable for keeping private and sensitive data. While there may be benefits, it is important to take into account possible hazards and abide by privacy and security laws. The blockchain itself is secure, but additional applications and layers are not. In terms of security, ML can aid in the development of blockchain applications. Therefore, a critical investigation is required to better understand the function of ML and blockchain in enhancing security. This study examines the current situation, evaluates the articles it contains, and presents an overview of the security issues. Despite their existing limitations, the papers included from 2012 to 2022 highlighted the importance of ML's impact on blockchain security. ML and blockchain can enhance security, but challenges remain; advances such as federated learning and zero-knowledge proofs are important, and future research should focus on privacy and integration with other technologies.

Keywords: blockchain; security analysis; machine learning; algorithms; applications

check for updates

Citation: Taherdoost, H. Blockchain and Machine Learning: A Critical Review on Security. *Information* **2023**, *14*, 295. https://doi.org/10.3390/info14050295

Academic Editors: Georgios Siolas, Kun She, Georgios Alexandridis and Paraskevi Tzouveli

Received: 23 March 2023
Revised: 25 April 2023
Accepted: 15 May 2023
Published: 17 May 2023

Copyright: © 2023 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Several fields in the real world have already begun to make use of and conduct extensive research into machine learning (ML) [1,2]. User-generated data in the tens of thousands per day may be utilized to train ML models, and those models can then be put to use solving a wide range of problems in business and society. Despite the progress of ML, data and model difficulties still exist. For instance, it is challenging to generalize ML models to reflect the future because current training methods require large amounts of data, which are often unavailable in practice [3] or limited due to the high cost of collection [4]. Concerns about data leakage and privacy [5] also exist. Filtering out "bad data" is a constant fight with malicious contributors or spammers, who can submit low-effort or illogical data and still receive rewards [6]. Additionally, it is difficult to generalize ML models to reflect the future due to outdated training [7], especially in subjects such as the Industrial Internet of Things (IIoT) [8], etc.

Most people agree that a blockchain is an efficient option that can guarantee security and reliability. However, as explained in [9], it may be vulnerable to attacks and security issues. Specifically, two significant attacks that undermined the network's functioning recently occurred on Ethereum Classic [10], a permissionless (public) blockchain-based decentralized platform for smart contracts [11]. The blockchain is defined roughly by a global ledger that can efficiently and permanently record transactions via a timed chain of blocks, or blocks. Each block is added to the chain after being validated, based on a distributed consensus procedure, and contains information about the transactions. When

Electronic copy available at: https://ssrn.com/abstract=4626844

enough nodes authenticate the block, which is subsequently regarded as reliable, the consensus is obtained. The whole procedure is recorded, and data may be gathered to describe the events taking place in the underlying ledger [12]. It is sensible to wonder whether such information may be used to monitor the process and provide early detection and analysis systems that can alert users to unusual events and potential attacks.

Data analysis techniques have historically been extensively used in the cybersecurity area [13], and the recent proliferation of powerful ML techniques has enabled the accurate identification of cyberattacks and the detection of threats, both in real-time and in post-incident assessments [14,15]. Importantly, both unsupervised and supervised ML algorithms have been used successfully to support the prevention and detection of intrusion systems, as well as detect system misuse and security breaches. The scenarios of interest are typically defined by a continuous data stream (such as application-level data or packet-level) summarizing the underlying network or system's activity. The role of ML algorithms is to recognize known threats (supervised technique) or aberrant behavior (unsupervised approach).

On the other hand, integrating blockchain may improve data quality, leading to better ML model training. As a result of the smart contract's validation process, harmful data that is unfavorable to model training will be filtered out, and researchers will not have to worry about having insufficient access to the most current data, which would lead to models that lack generalization. Data providers will also be protected from the unseen dangers of information security thanks to the encryption technology utilized by the blockchain. As blockchain and ML may be used to promote the creation of better ML models and make them more accessible to companies in fields such as supply chain, banking, healthcare, and so on, the combination will have far-reaching effects [16].

The blockchain can be specifically used to prevent cyberattacks and bolster the security of 5G applications. When compared to the consortium and private blockchains, the public blockchain is the most secure due to the nature of its participants and the consensus method used. While members of the consortium and private blockchains can only be trusted nodes, members of the public blockchain may be anonymous. The public blockchain uses Proof of Work (PoW) as its consensus technique, whereas multi-party voting and rigorously pre-approved nodes are used as consensus mechanisms in the consortium blockchain and private blockchain, respectively [17]. Blockchain has the unique ability to reduce cybersecurity threats, with its security characteristics including being very difficult for hackers or attackers to implant or distribute malware or harmful software. Blockchain increases the network's resilience by eliminating single-point failures and employs the consensus method, ensuring the ledger's transparency and integrity [18]. However, it is impossible to disregard some of the most significant blockchain security problems, including endpoint, scalability, a regulatory third-party vendor, and inadequate testing [19]. Another type of blockchain attack is the 51% assault, in which an attacker or group of attackers seizes control of the blockchain network [20]. ML algorithms are capable of analyzing transaction history and identifying patterns that indicate a possible double-spending attack. This can initiate an automatic response, such as suspending the account temporarily until the problem is resolved.

While ML and blockchain both hold enormous promise in a variety of businesses, their combination may potentially present new security issues that need to be resolved. The objectives of this review are to assess the present status of research in this field, pinpoint the biggest security issues, and suggest potential countermeasures. The blockchain itself is secure, but apps and extra layers are not. ML will benefit in the development of blockchain applications in terms of security. To the best of our knowledge, there is no security-focused evaluation of ML and blockchain. Therefore, a critical analysis is essential to comprehend the role of ML and blockchain in strengthening security and to provide insights to academics and practitioners working in this field. This research analyzes the current state of affairs, assesses the articles it includes, and provides an overview of security concerns.

Electronic copy available at: https://ssrn.com/abstract=4626844

2. Background

2.1. Security and Blockchain

There has been a significant surge in the number of reported security incidents involving the personal data of users. As a result, third parties may have access to the data and gather all personally identifiable information. This intermediary can be eliminated through the use of blockchain technology, which allows for direct transactions between two parties. The quantity of data in the environment has increased lately, and personal and sensitive information need not be safe in the hands of third parties as they are targeted for abuse and assault. Blockchain technology helps users who are not required to rely on a third party and acknowledges people as the owners of their data. However, it needs to have its regulations and norms, which is where the term "smart contract" comes in. Before initiating a transaction, the gateway keeper needs to draft a set of rules and a contract, which will facilitate peer-to-peer (P2P) interaction [21,22].

Many operations in cryptography are performed to provide various security services, including non-repudiation (ensuring authentication and integrity) [23], confidentiality (keeping information secret from communication parties), integrity, and authenticity. When asymmetrical cryptography is used, which has a set of public keys accessible to everyone and a set of private keys visible only to the owner, blockchain systems are naturally secure. These keys are used to ensure the integrity and ownership of a transaction [24,25]. The security of the blockchain system is linked to the integrity, confidentiality, and authorization of transactions. Unlike centrally kept data, which is more susceptible to security breaches, the decentralized structure of blockchain systems requires a P2P consensus mechanism, which reduces single points of failure for data [26]. There are many creative applications for blockchain, some of which are briefly discussed below. For example, Gai et al. [27] claim that integrating blockchain technology with an existing cloud solution could significantly improve the performance and security of cloud data centers. Recently, Wang et al. [28] implemented a secure and mutual authentication protocol to support the use of blockchain for identity verification issues in the smart grid. Similarly, before suggesting a blockchain-based authentication method for the smart grid, Wang et al. [29] highlighted a potential security threat to the infrastructure of the smart grid.

Despite the high level of security provided by blockchain systems, they are still vulnerable to various security and data integrity attacks [30]. PoW consensus-related attacks, such as 51% majority manipulation [31], consensus delay due to distributed denial of service [32,33], block ingestion, de-anonymization, blockchain forking, orphaned blocks, pollution log, and selfish mining [34], as well as attacks against double-spending [32] and liveness attacks [35] are some examples of these types of attacks. Based on the evidence, the majority of security issues arise from three primary areas: transactions, authentication, and network connectivity. Therefore, technologies that allow inappropriate connections and their integration with other technologies may pose several security risks [36]. Since the inception of blockchain technology, there have been five generations of technological advancements, and the range of applications has significantly expanded [37].

Blockchain security issues need to be addressed because, despite its potential benefits, blockchain technology introduces new security concerns that need to be addressed. Blockchain networks are decentralized, transparent, and immutable, which makes them a desirable target for malicious actors attempting to exploit system vulnerabilities [38]. A total of 51% of attacks, smart contract vulnerabilities, consensus algorithm flaws, and privacy concerns are some of the most significant security obstacles in blockchain networks. These security issues can result in data intrusions, monetary loss, and reputational harm for individuals and organizations that utilize blockchain networks. Consequently, it is essential to resolve these challenges through research and innovation to improve the security of blockchain systems and facilitate the pervasive adoption of this technology.

Electronic copy available at: https://ssrn.com/abstract=4626844

2.2. Blockchain and the Importance of ML

Through the usage of Bitcoin, blockchain [39] was largely promoted in the banking industry. It has been incorporated into many other sectors recently, including pharmaceutical manufacturing, supply chain operations, the healthcare sector, and many other important areas. Although ML is known for its automation of problem-solving by applying statistical computer algorithms or models, blockchain is often used for preserving financial transactions/data by maintaining a decentralized digital ledger that keeps all data in a highly safe manner.

In addition to processing enormous amounts of business data and building an effective prediction system that makes decisions automatically, ML is well known for its ability to analyze patterns in a dataset and interpret patterns in business data to produce excellent visual graphs and interpolations that can be used to provide insights into top management. In the insurance sector, cutting-edge ML algorithms have recently been utilized to predict financial risks. Insurance firms may accurately estimate the risks involved with charging new insurance premiums thanks to ML, which runs its algorithms on massive amounts of financial information and discovers a certain hidden pattern. Blockchain establishes a distributed ledger with a secure transactional database that has precise timestamps and immutable and permanent data instances. The main reason blockchain is so well-known is that it uses digital signatures as a particular method of reaching an agreement on financial data entities. Large amounts of data are needed for ML to produce credible models. Gathering, organizing, and auditing data is a straightforward approach made possible by blockchain that may increase data accuracy [40].

Blockchain greatly enhances data protection by automating the prediction of which types of data need to be stored and processed in a chain for making instances as accessible as possible. Blockchain has incredible support for standards for securing a lot of data at different nodes and makes data available at any instance in an encrypted manner. Since they are decentralized, blockchains may have security flaws [41]. The most prevalent issue is that the consensus procedure may be disrupted as a result of an assault, allowing a few mining farms to control which blocks are put into the network. This specific risk exists in public blockchains. Private versions are immune to this assault since each node is uniquely recognized, and a suitable consensus process is in place.

In the field of security, combining blockchain with ML may result in new and reliable solutions (Figure 1). For example, blockchain may be used to establish an immutable record of transactions that cannot be changed, and ML algorithms can be taught to identify patterns of fraudulent conduct in financial transactions. Blockchain may also be used to securely store data about network activities, and ML algorithms can be used to identify and stop cyberattacks in real time. ML may be used to validate users' identities based on biometric data, which can be utilized for identity verification. It is more difficult for hackers to obtain and use this data if it is securely stored in a decentralized way using blockchain. ML algorithms may be used to evaluate this data and find patterns of suspicious behavior or possible security breaches in supply chain security. Blockchain can be used to produce a safe and transparent record of every step in a supply chain. Lastly, ML can be used to analyze the behavior of these contracts and spot potential security flaws, helping to avoid the loss of money or other assets. Smart contracts are automatically executed based on predefined conditions and can be created using blockchain.

The adoption of blockchain technology in various industries has increased awareness of the significance of blockchain network security. By analyzing data, detecting patterns, and identifying potential security hazards in real time, ML has emerged as a potential method for enhancing the security of blockchain systems. By providing a secure, decentralized, and immutable digital ledger, blockchain can increase the veracity of data used by ML algorithms. However, blockchain networks are susceptible to security vulnerabilities, which necessitate the implementation of appropriate security measures and consensus procedures. The combination of blockchain and ML has the potential to revolutionize data security, but security needs to be maintained at all times.

Electronic copy available at: https://ssrn.com/abstract=4626844

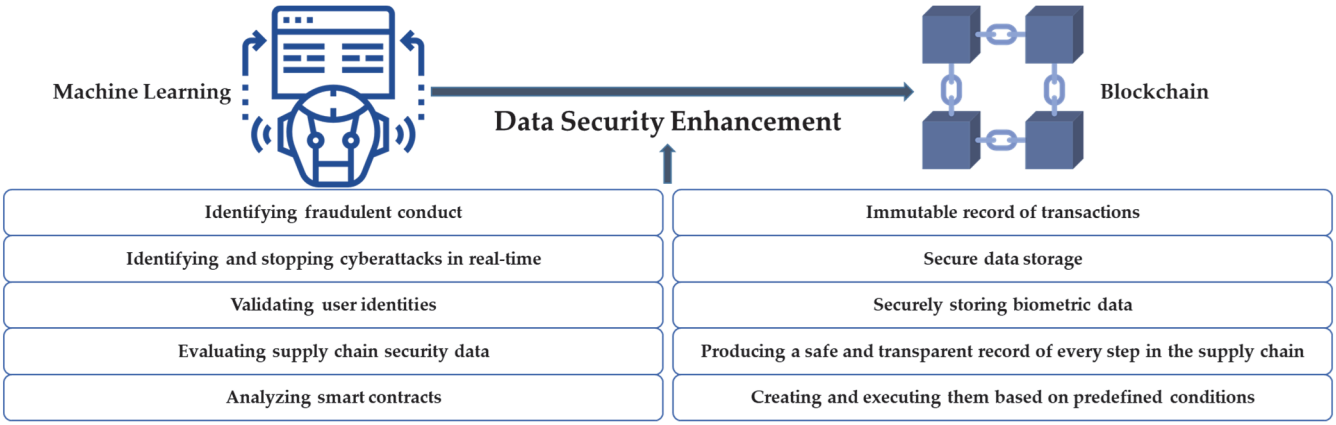
Machine Learning
Data Security Enhancement
Blockchain
Identifying fraudulent conduct
Identifying and stopping cyberattacks in real-time
Validating user identities
Evaluating supply chain security data
Analyzing smart contracts
Immutable record of transactions
Secure data storage
Securely storing biometric data
Producing a safe and transparent record of every step in the supply chain
Creating and executing them based on predefined conditions

Figure 1. ML method to enhance data security of blockchain.

3. Methods and Materials

3.1. Research Method

In recent years, security studies literature has expanded as an increasing number of academics have taken an interest in the topic. By using the AND OR search operators, a great quantity of relevant material on themes such as "Machine Learning", "Security", and "Blockchain" can be located. On 9 March 2023, 33 articles remained from 369 ones (Figure 2).

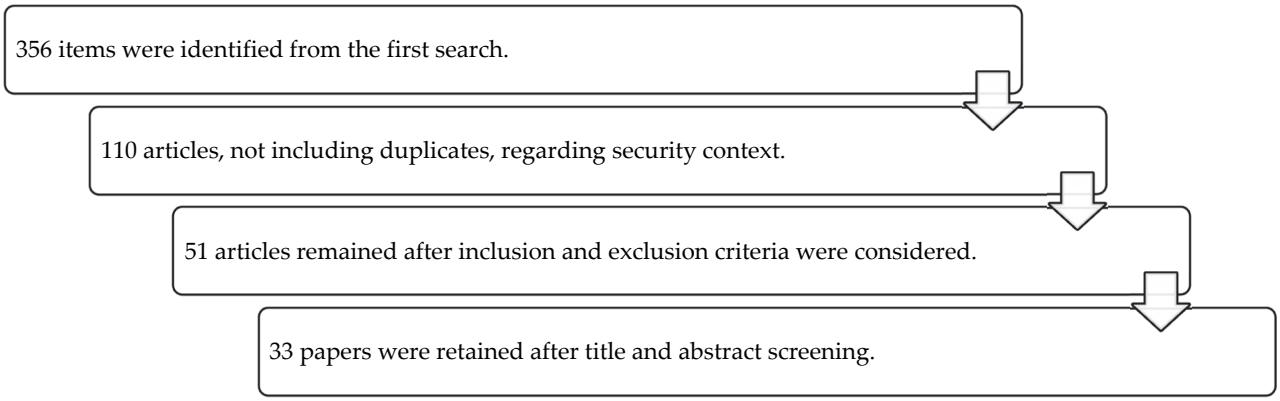
356 items were identified from the first search.
110 articles, not including duplicates, regarding security context.
51 articles remained after inclusion and exclusion criteria were considered.
33 papers were retained after title and abstract screening.

Figure 2. Document selection process.

Keywords:

- "Machine Learning" AND "Blockchain" AND "Security"
- "Machine Learning" AND "Blockchain" AND "Network Security"
- "Machine Learning" AND "Blockchain" AND "Security of Data"
- "Machine Learning" AND "Blockchain" AND "Cybersecurity"
- "Machine Learning" AND "Blockchain" AND "Security and Privacy"
- "Machine Learning" AND "Blockchain" AND "Privacy and Security"

3.2. Exclusion and Inclusion

Using "blockchain" and "machine learning" as keywords in the context of security, papers were located in the Scopus, Google Scholar, and Science Direct databases. These studies include research on machine learning categorization, security, and the integration of blockchain with machine learning. Figure 3 outlines the inclusion and exclusion criteria that need to be met by research papers chosen for this study's critical examination.

Electronic copy available at: https://ssrn.com/abstract=4626844

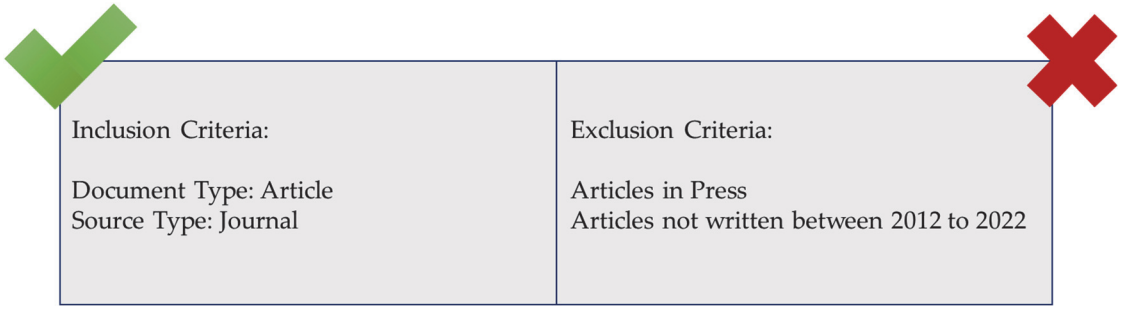

Figure 3. Inclusion and exclusion criteria.

3.3. Study's Objective

The primary aims of this research are as follows:

- To understand the literature on ML and blockchain applications for security
- To understand the significance of ML.
- To understand the many solutions to these problems.
- To understand the open issues, challenges, and future directions of research.

4. Current State of Scope

The number of articles on ML and blockchain in the context of security has steadily increased over the previous four years from 2012 to 2022. Figure 4 shows the yearly number of papers published by topic area from 2012 to 2022. The chart below shows how publishing dates have changed over time: in 2019, three papers (9.10%) were published, nine articles (27.27%) in 2021, and twenty-one articles (63.63%) in 2022. It is important to note that there has been a huge increase in the use of blockchain and ML, particularly in 2022. The most published research in this area occurred in 2022. Due to the expanding use of these technologies across a variety of industries, concerns about potential security threats, and improvements in ML methods and blockchain protocols that open up new avenues for innovation, publications on the intersection of blockchain and ML in the context of security have grown over time. As a result, experts in both fields are working hard to find methods to make blockchain and ML applications more secure.

The key disciplines are computer science (30 articles) and engineering (19 articles). The majority of publications on the intersection of blockchain and ML in the context of security are in the computer science and engineering areas due to the close relationship between the implementation and development of these technologies, the importance of security, and the interdisciplinary nature of the research that requires expertise in multiple fields. These disciplines provide the foundation for developing blockchain and ML algorithms, and concentrate on the practical implementation of these algorithms in real-world applications, making them well-suited for investigating and proposing solutions to security problems.

There is a growing trend of producing essays on various topics. The use of ML to control the blockchain can greatly enhance the security of the chain. Furthermore, since ML performs better with large amounts of data, it presents an excellent opportunity to create stronger models by leveraging the decentralized nature of blockchains. When combined, ML and blockchain can enhance security and transparency. This integration can be particularly beneficial for small businesses that cannot afford significant maintenance costs. Maintenance schedules can be posted on the blockchain, ensuring that everyone is accountable for their specific responsibilities.

Electronic copy available at: https://ssrn.com/abstract=4626844

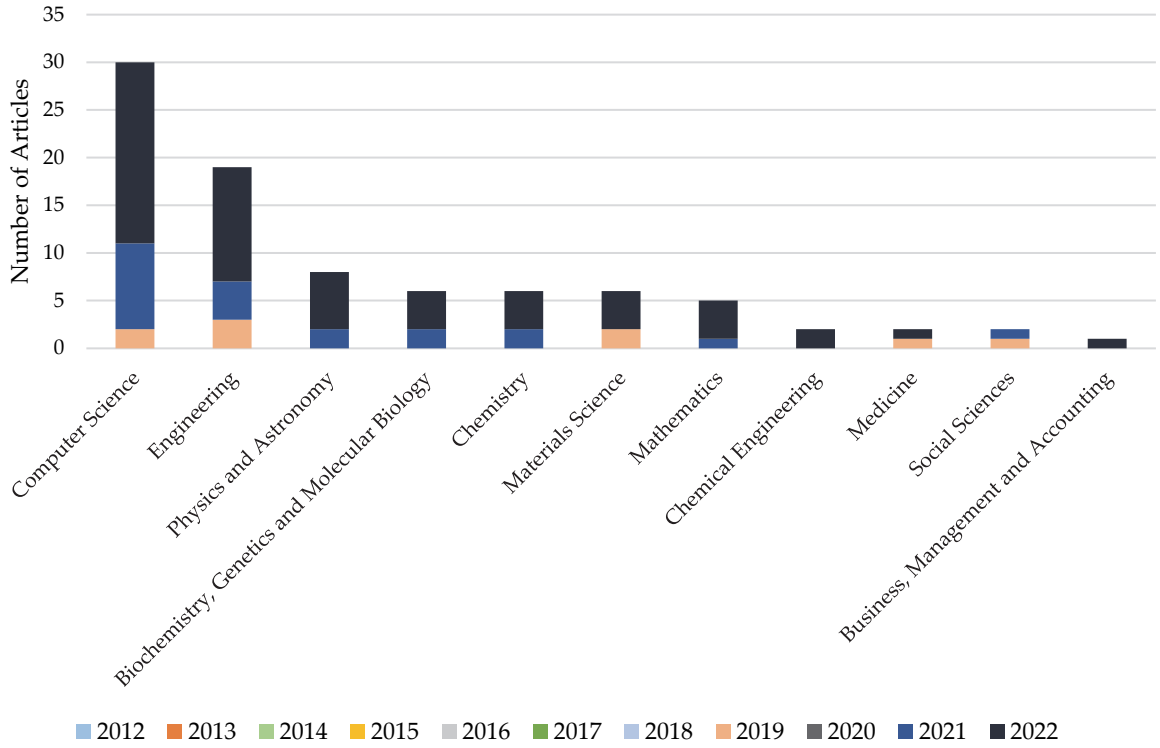

Figure 4. The number of topical articles written between 2012 and 2022.

5. Discussion

Integrating block chain with ML can make data storage and processing more efficient and beneficial for data management. For example, Gaur et al. [42] presented an ML-based blockchain smart-contract system that enhances security, decreases consumption, and can be relied upon for real-time medical applications. Additionally, models based on the blockchain can use ML algorithms for data prediction and analysis to enforce security and identify threats [43]. ML techniques are also beneficial in cybersecurity and can be used for defending against distributed denial-of-service (DDoS) attacks. Several ML-based approaches for identifying DDoS attacks have been proposed, including supervised, unsupervised, and hybrid approaches that combine the first two [44]. Another example is the project by Shahbazi and Byun [45], which aims to build a system for disaster management and emergency response based on social media platforms. This approach uses text analysis techniques to improve how authorities respond to emergencies and filter the information using automatically-collected data to aid in relief efforts. The project extracted real-time information linked to emergencies from social media datasets using cutting-edge ML, Deep Learning, and Natural Language Processing approaches based on supervised and unsupervised learning to assist in quick reaction in a crisis. Similarly, blockchain architecture is used in this procedure to disprove the veracity of specified events and get rid of the system's exclusive authority. The integrated system is primarily motivated by the need to increase system transparency and security to prevent the dissemination of incorrect information on an event on social media. Furthermore, as a fast-evolving technology, ML has been recommended as a software engineering security analysis tool [46].

Security is crucial not only for the continued use of blockchain but also for data distribution due to its faster operation [47]. In a recent paper, Al-Qarafi et al. [47] presented the Optimal ML-based Intrusion Detection System for Privacy-Preserving BIoT with Smart Cities Environment (OMLIDS-PBIoT) approach, which is a solution for achieving smart city environment security using blockchain and ML techniques. To achieve this, the OMLIDS-PBIoT approach uses initial data pre-processing to convert the data into a suitable format. It also employs a golden eagle optimization (GEO)-based feature selection model to extract valuable feature subsets and a heap-based optimizer with a random vector functional

Electronic copy available at: https://ssrn.com/abstract=4626844

link network model for intrusion categorization. Furthermore, the IoT-enabled smart city environment utilizes blockchain technology for secure data transfer. The performance of the OMLIDS-PBIoT method is validated using benchmark datasets, and the results are examined under a variety of conditions. The experimental findings suggest that the OMLIDS-PBIoT technology is superior to contemporary techniques. Using hybrid deep-learning classification techniques may further enhance the efficiency of the OMLIDS-PBIoT methodology.

As the number of smart devices continues to rise, privacy breaches and poor model accuracy of edge services ensue [48]. Tian et al. [48] propose a blockchain-based ML framework for edge services (BML-ES) in IIoT to address these issues. Specifically, they develop unique smart contracts to enable multiparty engagement of edge services to increase data processing efficiency. To ensure the accuracy of decision tree (DT) models, they also provide an aggregation approach to verify and aggregate model parameters. In edge services, they guarantee data security and prevent data leakage by using the SM2 public key cryptosystem. Theoretical simulations and analytical studies have shown that the BML-ES architecture is better suited for enhancing the accuracy of edge services in the IIoT. It is secure, efficient, and effective. However, the security and effectiveness of data processing utilizing ML still differs significantly [49,50]. The elliptic curve discrete logarithm problem in SM2 is largely responsible for the security of BML-ES. Their solution is protected by this feature against data loss and tampering [48].

The categorization of included studies based on applications, protocols, algorithms, and security analysis is a method for organizing and comprehending the enormous quantity of available literature in a given field. This classification can also enable the identification of gaps in the research that require further investigation, which can help guide future research in the field. Ultimately, this categorization of research papers is a practical method for comprehending the vast amount of literature in a given field, and it plays a crucial role in advancing knowledge and improving research outcomes in computer science, information technology, and cybersecurity.

5.1. Applications

Recent research suggests that ML and blockchain have significantly impacted the security of industrial automation over the past few decades. Blockchain is an immutable list of files that are linked cryptographically and available for inspection, the same as a ledger. It makes it impossible to modify prior accounting ledger papers, and fresh documents need to be hacked by a trustworthy source. Permissioned blockchains use a variety of cryptographic methods, including elliptic symmetric cryptography and the curve digital signature algorithm, to protect the security of data. The proposed system can include e-commerce and risk management activities in addition to the traceability of industrial equipment. Rather than just detecting harmful flow rules, it is exciting to utilize the blockchain to prevent their introduction into flow tables [51]. To evaluate the accessibility, dependability, privacy, and security of the ePrescription information in the proposed system, a survey covers questions on the ePrescription system's properties [52]. The survey by Aldughayfiq and Sampalli [52] revealed that a great majority of respondents across all demographics viewed the use of blockchain and ML algorithms to securely prescribe pharmaceuticals favorably. Nevertheless, minor enhancements are required for the suggested functionalities, and post-implementation user research is required to assess the proposed ePrescription system in full.

Smart cities are becoming the norm in urbanization due to the growth of IoT. IoT networks allow dispersed smart devices to collect and analyze data within smart city infrastructure using the Internet as an open channel. However, challenges such as centralization, scalability, transparency, privacy (such as inference attacks and data poisoning), security, and verifiability slow down the adoption of smart cities [53]. Inspired by these challenges, Kumar et al. [53] offer a privacy-preserving and secure framework (PPSF) for smart cities powered by the IoT. The proposed PPSF relies on two fundamental mechanisms: a two-

Electronic copy available at: https://ssrn.com/abstract=4626844

level privacy strategy and an intrusion detection technique. A blockchain module is first developed in a two-level privacy system to transport IoT data securely, and the Principal Component Analysis (PCA) method is utilized to reformat the raw IoT data. Using the ToN-IoT and BoT-IoT network datasets, a gradient boosting anomaly detector is employed in the intrusion detection method to train and evaluate the proposed two-level privacy solution. For the implementation of the suggested PPSF framework, they additionally provide a blockchain-integrated Fog-Cloud architecture with an InterPlanetary File System (IPFS). According to the testing results, the PPSF architecture is superior to certain modern blockchain and non-blockchain alternatives.

Ensuring secure and confidential communication in the IoT is a challenge, given its expected size and widespread usage. Blockchain has been explored as a potential solution for decentralized privacy and protection. However, existing methods are computationally and temporally intensive, making them impractical for most IoT applications [54]. Particularly, Khan et al. [54] propose a resource-efficient blockchain-based approach for private and secure IoT. They use the Deep extreme learning machine instance and novel exploitation of computing resources in a typical IoT context, such as smart homes. Their suggested method involves safeguarding blockchain-based smart home architecture by assessing its dependability on accessibility, integrity, and privacy. Simulated results demonstrate that the overheads introduced by their strategy (in terms of energy consumption, processing time, and distribution) are insignificant compared to their protection and privacy advantages.

In China, the adoption of national standard cryptography is being promoted for security applications. Yi [55] suggests a blockchain-based instant messaging system with a Chinese cryptographic foundation. To prevent counterfeit and replay attacks, he builds a message authentication scheme based on SM2, followed by an SM3-based cryptographic hash mode for message integrity verification. He then builds an SM4-based message encryption mechanism to protect user privacy. Additionally, he presents an algorithm-based strategy for monitoring blockchain activity to detect anomalies. To prove the feasibility of the blockchain-based IM scheme, a Linux-based blockchain-based IM system was developed. The implementation results demonstrate that it is a secure and realistic IM system that can be implemented directly on a wide range of instant messaging apps.

This section outlines various potential applications of blockchain and ML for enhancing security and privacy in diverse contexts. However, the authors acknowledge that more research and user trials are needed to evaluate the full potential and functionality of the proposed systems. Moreover, it is crucial to note that the implementation of such systems may face challenges related to verifiability, transparency, scalability, and centralization, as discussed in the text. Table 1 highlights the potential uses of the articles described in several fields, including industrial automation, IoT-powered smart cities, secure IoT connectivity, and instant messaging. This table rates each application according to its benefits and challenges.

Table 1. Potentials for enhancing security with advantages and challenges.

Application	Advantages	Challenges	References
Industrial automation security	Cryptographic protection of data and immutability	Functionality requires minor enhancements, and post-implementation user research is required.	[51,52]
Smart cities powered by IoT	Superior performance, security, and privacy preservation	verifiability, privacy, transparency, scalability, and Centralization	[53]
Secure communication in IoT	resource efficiency and decentralized privacy protection	The computational and temporal intensity of existing methods	[54]
Instant messaging	Anomaly detection, integrity verification, privacy protection, and message authentication	Implementation obstacles include verifiability, transparency, scalability, and centralization.	[55]

Electronic copy available at: https://ssrn.com/abstract=4626844

5.2. Protocols

Conventional learning techniques rely on the system's trust for confidentiality and security. However, as the scale of learning expands, maintaining the integrity of every edge device may become expensive [56]. Zhang et al. [56] proposed democratic learning (DemL) to cost-effectively develop trust in a trustless environment. The investigation into hardware/software co-design for decentralized, blockchain-secured, on-device learning has reached this stage. Their method protects artificial intelligence (AI) learning in a trustless environment by using blockchain's decentralization and tamper-resistance. They suggest PoMC (an algorithm and architectural co-design) as a special blockchain consensus mechanism that makes use of cross-domain reuse (AI learning and blockchain consensus) for the first time in AI learning architecture to offset the extra cost that a blockchain provides. According to the assessment results, their DemL can shield AI learning from privacy leakage and model contamination, and privacy and security are only marginally accompanied by hardware overhead and power consumption (2%).

In addition, by integrating blockchain into a cloud computing environment, a new framework for managing trust will increase the efficiency and authentication of cloud servers. This hybrid cloud-based blockchain architecture is referred to as blockchain as a service (BaaS) [57]. Franklin et al. [57] proposed a framework that includes a smart contract and access mechanism for authenticating data against Byzantine attacks. The efficacy of the suggested model is compared to several state-of-the-art methodologies, demonstrating that their framework provides the best level of protection against Byzantine attacks. The blockchain is responsible for generating and storing transaction data inside blocks. TBB is responsible for collecting the most recent transactions from each node and generating transaction blocks before validating their behavior and creating behavior trust blocks. The details are then transmitted to TAB. TAB and TBB are the two primary blockchain data security protocols.

Moreover, to optimize the blockchain-intersected IoT system, a light chain consensus reinforcement ML (LCC-RML) approach was created by Priyadharshini and Canessane [58]. This approach contributes to the development of a learning technique from the angles of resource utilization, decentralized data security, scalability, and latency. The underlying blockchain technology in LCC-RML has improved scalability without affecting the decentralized system, latency, or security. To improve network Quality of Service (QoS) and security, the sidechain is established using a modified two-way peg process and updated using a hybrid delegated useful Byzantine fault tolerance-delegated proof of stake (DPBFT-DPOS) method [59]. The suggested technique by Vairagade and Brahmananda [59] obtains an accuracy and (Formula given)-score of around 98.6% and 99.5%, lowers end-to-end communication time by 10%, enhances energy efficiency by 15%, and increases throughput by 15% relative to current methods.

To address security issues and overcome the limits of current methodologies, Zhou et al. [46] suggested using a tree-based ML vulnerability detection (TMLVD) method to analyze the vulnerabilities of smart contracts. TMLVD sends intermediate representations of smart contracts made from abstract syntax trees to a tree-based training network to build the prediction model. To find smart contract vulnerabilities, their method collects multidimensional properties. The results indicate that TMLVD has sufficient detection capabilities for locating specific security vulnerabilities.

Vargas et al. [60] aimed to merge prior methods to provide a comprehensive security mechanism for IoT device networks. Their mechanism would enable the detection of threats, activate secure information transmission mechanisms, and be tailored to the computing capabilities of industrial IoT. Considering the prior assumption and the fact that the IIoT security exploits have been detected, they selected the K-nearest neighbors algorithm (KNN), a supervised ML technique that only needs a distance calculation between nodes. The suggested approach achieves the specified goals and provides a realistic mechanism for identifying and containing intrusions in an IoT network. In some instances, it evades conventional detection measures, such as an intrusion detection system.

Electronic copy available at: https://ssrn.com/abstract=4626844

Choudhary and Dorle [61] used a delay-aware, energy-aware, throughput-aware, and PDR-aware underlying protocol to execute routing, security, and network parameter tuning, which employs high-efficiency ML. In comparison to the traditional blockchain-based vehicular ad-hoc network (VANET) implementations, this resulted in a 12 percent decrease in energy usage, a 15 percent decrease in E2E latency, and a 38 percent boost in network throughput. The network packet delivery ratio (PDR) is almost constant and can be enhanced by using deep learning and ML models, such as long short-term memory (LSTM) and convolutional neural network (CNN) architectures, by providing more weight to PDR enhancement. In addition, the underlying network employs a sidechain-based blockchain implementation, making it less complicated, more secure, and faster than single-chain implementations. In the future, researchers may extend this protocol to increase secondary characteristics such as parametric jitter, routing overhead, cost of storage, and computational complexity.

A concept called Secure LearningChain (SEC-LearningChain) was presented by Pon and Kavitha [62], based on a combination of blockchain, ML, and cloud computing primitives. It aims to provide secure data transactions in a P2P network and an efficient data-sharing service. This strategy comprises four design models: Firstly, an attack detection model uses a threshold-based abnormal traffic detector in the transaction network to identify attacks. Secondly, a blockchain transaction network architecture based on cryptographic hash and encryption is designed to combat threats and authenticate the identity verification procedure for safe transactions. Thirdly, the large-scale transaction record is optimized, and the ML output prediction model is trained. Lastly, the cloud assessment model controls the saved transaction records and facilitates the easy sharing of accessible services across various cloud systems for each service center. Additionally, they demonstrate that the SEC-LearningChain architecture is resistant to transmission control protocol flooding, denial of service, and fake attacks. Experimental findings indicate that the SEC-LearningChain achieves a greater number of transactions per block than previous systems.

ML can aid in preventing tampering issues during runtime and beforehand [63]. In the study by Nasir et al. [63], the suggested framework used various ML approaches; however, support vector machines (SVM) outperformed the others, achieving 99.05% DA and 0.95% MCR (enabled by blockchain) to overcome security risks to trained models, network communication, transaction data. In the future, federated ML augmented with fuzzy data may be used to solve further network interference issues. Unal et al. [64] suggest using blockchain to protect IoT systems against federated learning (FL) algorithm assaults. Combining blockchain and FL safeguards the integrity of trained models, avoiding model poisoning threats. This study proposes a viable method for integrating blockchain with FL to deliver secure and private big data analytics services. To safeguard trained models and user data against poisoning attempts, they suggest using fuzzy hashing to identify variations and abnormalities in FL-trained models. The suggested solution is assessed by modeling attack modalities in a quasi-simulated environment.

Despite the presentation of promising protocols that use blockchain and ML technologies to improve security, scalability, and privacy in decentralized systems, further research and evaluation are required to determine the efficacy and viability of these protocols in real-world settings. When designing and implementing such protocols, it is essential to consider the tradeoffs among security, performance, and usability. Table 2 provides a comparison of various protocols based on their advantages and applications of included works.

5.3. Algorithms

ML algorithms are commonly used to study observations by identifying data patterns, mapping input to output, and analyzing data. As these algorithms analyze more data, their overall accuracy in predicting outcomes improves. New iterations of existing ML algorithms continue to emerge depending on the shifting needs and complexity of the issues.

Electronic copy available at: https://ssrn.com/abstract=4626844

Table 2. Comparison of different protocols.

Protocol	Advantages	Applications	References
DemL	Cost-effective trust in an environment devoid of trust and protection against privacy leakage and model contamination	AI learning	[56]
BaaS	Superior level of defense against Byzantine attacks	Cloud computing	[57]
LCC-RML	Scalability, latency, and security are enhanced without compromising the decentralized system.	IoT systems	[58,59]
TMLVD	Adequate detection tools for identifying particular security flaws	Smart contracts	[46]
KNN	A practical method for locating and containing intrusions in an IoT network	IoT device networks	[60]
Delay-Aware, Energy-Aware, Throughput-Aware, and PDR-Aware Underlying Protocol	Reduced energy consumption and E2E latency, enhanced network throughput	VANET	[61]
SEC-LearningChain	Secure data transactions and effective service for sharing data	P2P network	[62]
SVM	Enhancing the protection of trained models, network communications, and transaction data	Runtime and beforehand security in ML	[63]
Federated ML with fuzzy data and Blockchain	Protecting the integrity of trained models, preventing model poisoning, identifying anomalies, and secures IoT systems	Secure and private big data analytics services	[64]

In the study by Shahin and Sabri [65], the authors present a framework for safely storing IoT data while maintaining its integrity and availability. Multiple ML algorithms, including Naive Bayes, AdaBoost, KNN, DT, Random Forest, and Logistic Regression (LR), are trained to identify hacked IoT devices. These algorithms are compared based on metrics such as recall, accuracy, precision, F1 score, and classification time. The findings suggest that Random Forest and AdaBoost classifiers provide similar results and are considered the top classifiers based on all performance criteria, except for time. After filtering, typical data received from IoT devices are stored on a private blockchain, and the signed data are subsequently sent to all network nodes for verification. The blockchain's consensus process is built on the proof of authority algorithm to enable scalability.

Similarly, the architecture created by Jamil et al. [66] provides an innovative solution for securing IoT fitness gadgets. This secure architecture includes data security, restricted access to fitness devices, and the consensus method (PBFT), which allows IoT fitness device fault tolerance. The blockchain's data decentralization and encryption capabilities ensure data security for IoT devices. The proposed system is evaluated using well-known ML-based classifiers such as KNN, SVM, LR, and DT. The capability of smart contracts increases confidence in IoT fitness gadgets and reduces potential costs. Asymmetric encryption is considered the primary technique used to protect the security of the blockchain. Asymmetric encryption, which uses a public and private key, is used to offer digital signature and data encryption features. In addition to providing transaction verification and signatures, asymmetric cryptography secures the security of IoT fitness data in the blockchain. The primary purpose of blockchain is to securely record data into blocks, with each transaction confirmed by other nodes within the blockchain system.

Electronic copy available at: https://ssrn.com/abstract=4626844

Distributed ML (DML) has been researched by Kim et al. [67] for blockchain networks as a way to operate a learning model without data centralization. Despite various works being offered, privacy and security have not been adequately addressed. Therefore, Kim et al. propose a privacy-preserving DML paradigm for a permissioned blockchain to systematically address performance, security, and privacy challenges. They create a differentially private stochastic gradient descent technique and an error-based aggregation rule as fundamental primitives for any differentially private technique for learning, in which non-deterministic functions need to be specified. The suggested error-based aggregation rule is effective in preventing attacks by an adversary node that attempts to reduce the precision of DML models. Their results indicate that their suggested approach offers more resistance against adversarial attacks than existing aggregation procedures in a differentially private setting. Lastly, they demonstrate that the suggested model is useful due to its low computing cost and transaction latency.

Shahbazi and Byun [68] tested several ML and blockchain-based approaches to multi-stage quality control. They provide the cross-validation test results, which are separated into accuracy, precision, and recall for the gradient tree boosting technique (XGBoost) and KNN algorithms. XGBoost had the most influence on the proposed strategy and has been compared to various ML techniques. Comparing XGBoost to various ML algorithms revealed that XGBoost can extract the complicated connection of the dataset and deliver the most accurate quality rating. The primary objectives and innovations of the described system were to use a blockchain coupled with ML to enhance smart manufacturing practices and environmental quality, delivering exceptional results. This technology provides a secure environment for producers and users to enhance the safety and reliability of corporate settings. In future work, they can expand the network size to test and evaluate the system's performance in more complex production contexts concerning precision, ML models, etc.

In Korea, one of the prevalent modes of transportation is the use of internet apps to hail taxis, which is more convenient for drivers and passengers. However, the driver's taxi request for passengers may be denied depending on the driver's position and distance. Therefore, the driver's rejection and acceptance of the received request needs to be specified. To preserve transaction information and ensure the safety of passengers and drivers, the security of this system is another essential component [69]. In the work by Shahbazi and Byun [69], the origins and destinations of visitors to the South Korean island of Jeju were extracted from T-map data and processed using ML DT and XGBoost algorithms. The blockchain structure is built on the Hyperledger Fabric platform. The suggested framework increases the security of passenger transaction data and decreases passenger waiting time at the specified site.

The paper by Kumar et al. [70] presents a trustworthy privacy-preserving secured framework (TP2SF) for smart cities, which is composed of three modules: an intrusion detection module, a privacy module with two levels, and a trustworthiness module that creates a blockchain reputation platform. To guard against inference and poisoning attacks, the privacy module uses a blockchain-based improved proof-of-work (PoW) technique in conjunction with PCA to transform data into a new reduced shape. XGBoost is used in the intrusion detection module. They recommend using the CloudBlock and FogBlock infrastructure, which is a blockchain-IPFS integrated Fog-Cloud infrastructure, for implementing the TP2SF framework in smart cities due to the advantages and drawbacks of the Fog-Cloud architecture. The TP2SF framework is evaluated using two real IoT-based datasets, ToN-IoT and BoT-IoT, and is found to outperform other cutting-edge approaches in both blockchain and non-blockchain systems.

Researchers have presented security models based on blockchain, and these models enable high-speed operations for small-scale networks. Nevertheless, as network size rises, the latency required for blockchain mining increases exponentially, limiting its use [71]. The work by Agrawal and Kumar [71] proposes an ML-based blockchain architecture called MLSMBQS for QoS-aware secure IoT installations that utilizes bio-inspired computing to

Electronic copy available at: https://ssrn.com/abstract=4626844

split the blockchain into many sub-chains, referred to as shards, to reduce mining time. The suggested model is capable of increasing throughput, decreasing communication latency, reducing energy usage, and enhancing security performance compared to current blockchain and non-blockchain-based security models. Thus, the MLSMBQS model is deployable in a range of IoT network situations requiring high efficiency.

Several ML algorithms, including Naive Bayes, AdaBoost, KNN, DT, Random Forest, SVM, LR, and XGBoost, have been studied for their effectiveness in enhancing the security and privacy of blockchain-based systems in a variety of applications. However, the different research aims, target applications, and assessment standards make it difficult to evaluate the effectiveness of ML algorithms across investigations. Additionally, some studies may be subject to constraints such as small sample numbers, a lack of data variety, or inherent biases in data collection and preparation. Table 3 summarizes the algorithms used, the proposed solutions, and the evaluation metrics used to assess the performance of the proposed systems.

Table 3. Overview of ML algorithms and blockchain applications in various fields.

ML Algorithms Used	Objective	References
Naive Bayes, AdaBoost, KNN, DT, Random Forest, LR	Safely storing IoT data while preserving its availability and integrity	[65]
KNN, SVM, LR, DT	Securing IoT fitness gadgets	[66]
DML	Operating a learning model without data centralization	[67]
XGBoost, KNN	Multistage quality control	[68]
ML DT, XGBoost	Enhancing the safety of passenger transaction data and reducing waiting time	[69]
XGBoost	Providing the TP2SF for smart cities	[70]

5.4. Security Analysis

Blockchain and ML systems both require a high level of security to prevent malicious attacks and data breaches. Hence, the security analysis is crucial for both of these technologies. Security analysis in ML entails identifying potential weak points in the architecture and creating defenses against prospective threats. ML models, for instance, are susceptible to adversarial attacks, in which a perpetrator modifies input data to trick the model and produce false predictions. These vulnerabilities can be found, and effective protections against them can be created with the aid of security analysis.

Similarly, the security analysis is essential in blockchain systems to prevent unauthorized access and maintain the integrity of the distributed ledger. Blockchain systems rely on cryptographic algorithms for the authenticity and immutability of transactions. However, these algorithms can be vulnerable to attacks such as 51% attacks, in which an attacker seizes control of the majority of the network's processing capacity and manipulates the ledger. These vulnerabilities can be found, and solutions to reduce the risk of attacks can be developed with the use of security analysis. Additionally, security analysis can assist in identifying weaknesses in the hardware and software components of blockchain and ML systems. For instance, a flaw in the hardware of a blockchain system might be leveraged to take over the network, or a weakness in a third-party library or component used in an ML system might be exploited to gain unauthorized access to sensitive data.

Blockchain technology is being used more widely, but as its popularity has grown, so too have new attack techniques. For instance, exchanges have been targeted, and there are reports of increasing numbers of digital currencies being stolen [72]. Therefore, it is essential to conduct security analysis on both ML and blockchain systems. However,

Electronic copy available at: https://ssrn.com/abstract=4626844

it is important to note that security analysis should not focus only on the limitations of cryptographic methods but also encompass people and procedures.

To improve the credibility of website defacement detection and lower false-positive and false-negative rates, Du et al. [73] proposed an ML and blockchain-based method for fine-grained trust detection called WebTD. Their testing findings and security analysis demonstrated that WebTD not only builds a trustworthy web service detection system, but also maintains a detection success rate of over 98%, ensuring the website's integrity.

Table 4 contains several publications that examine security analysis in both blockchain and ML systems. Overall, it is clear that security analysis is critical to ensuring the integrity and trustworthiness of these technologies. Security analysis involves a range of techniques, such as threat modeling, vulnerability assessment, penetration testing, and risk analysis, and should be an integral part of any system design or implementation.

Table 4. Overview of some articles that study security analysis.

System	Method	Outcome	Limitation	References
ML Technique and Consortium Blockchain	Oyente	Enhancing the security and confidentiality of transactions	Using their recommended model in a real-world setting without comparing it to other charge schemes with the same characteristics.	[74]
ML and Blockchain	Oyente	The suggested method detects transaction fraud correctly.	Is susceptible to the adversary's attack	[75]
Exploiting ML in Intelligent Sensor-Based Systems Using Blockchain	Oyente	The smart contract is resilient against flaws.	When a function is run, it prevents the execution of other functions.	[76]
Data Trade Mode Based on Smart Contracts Utilizing Blockchain and ML	Not mentioned	Addressing the issue of the data trading center's inability to keep data in the conventional data trading mode, to preserve the data owner's rights and interests and support the growth of data trading.	The remedy to the issue of data resale is to sign a non-resale contract, although signing a contract cannot remove the problem of data resale.	[77]

6. Open Issues and Future Directions

In the future, ML and blockchain have the potential to revolutionize security. However, to actualize their maximum potential in security, it is necessary to resolve several outstanding issues and obstacles. ML algorithms may also be susceptible to adversarial attacks, in which an adversary modifies data to induce algorithmic errors. Additionally, the following factors need to be addressed in future research:

- Scalability: Blockchain technology is still comparatively sluggish and has difficulty processing large quantities of data. In addition to being computationally intensive, ML algorithms can make it difficult to process data swiftly and effectively.
- Interoperability: Due to numerous blockchain platforms and standards, it can be challenging to develop interoperable systems that are compatible with multiple platforms.
- Privacy: Blockchain technology can produce a transparent and unchangeable ledger of transactions, which can raise privacy concerns. In addition to collecting vast quantities of data, ML algorithms can also raise privacy concerns.

Numerous noteworthy advancements have been made in the field of emerging trends and technologies. Federated learning is one of these innovations, as it permits multiple parties to train a shared model without revealing their data. This could be advantageous for refining ML models on blockchain-stored data without revealing the data to third parties.

Electronic copy available at: https://ssrn.com/abstract=4626844

Another notable technology is zero-knowledge proofs, a cryptographic technique that allows one party to establish the veracity of a statement without revealing additional information. This could be used to authenticate information without revealing the information itself. Interledger protocols permit the development of interoperable systems by facilitating communication between diverse blockchain platforms. These protocols could be utilized to establish a secure and decentralized network for inter-blockchain communication, enabling blockchain platforms to share data and interact. Moreover, tokenization can be used to generate digital tokens that represent physical assets. Then, ML algorithms can be used to identify activity patterns associated with these identifiers to detect potential fraud or other security issues.

Further research on privacy-preserving methods, such as federated learning, might be one of the field's future goals. This would help to solve issues with data ownership and security. There may also be opportunities to enhance the effectiveness and scalability of ML algorithms for usage in blockchain networks as well as to create novel consensus mechanisms that can satisfy the particular requirements of ML-based applications. Finally, there may be opportunities to investigate the fusion of other cutting-edge technologies, including edge computing and natural language processing, with ML and blockchain to develop fresh and cutting-edge solutions for a variety of sectors and use cases.

7. Conclusions

Nowadays, blockchain is considered the most cutting-edge and trustworthy technological framework for investigating a wide range of security-related problems. Unlike the immutable ledger that serves as the backbone of all cryptocurrencies, ML is a rapidly growing field that promises endless applications. By optimizing blockchain with ML, it might be possible to achieve greater efficiency. Information stored on a blockchain is secure because of its built-in encryption, making blockchains great for storing secret or sensitive information. However, enhancing security entails much more than that. While the blockchain itself is secure, any additional programs or layers on top of it are not. To improve the safety of blockchain applications, ML can be of great help. Our research has not revealed any kind of security-oriented assessment of ML with blockchain. Therefore, a comprehensive study is required to understand the function of ML and blockchain in enhancing security. This study evaluates the current situation, ranks the included papers, and presents an overview of security issues.

Since 2019, a growing number of papers have focused on the security implications of ML and blockchain technology. It is important to recognize the meteoric rise of ML and blockchain technology, particularly in 2022. The distributed ledger used by blockchain can be made more secure with the help of ML. Computer science and engineering are key to this. The trend of writing essays in many disciplines is expanding. When applied to blockchain management, ML has the potential to further strengthen the network's already impressive security. In addition, the decentralized structure of blockchains provides a tremendous opportunity to build stronger models, which is especially appealing given that ML performs better with vast volumes of data. Together, they make the world a safer and more open place. In certain cases, it might be highly useful to combine ML algorithms with blockchain. The featured publications highlighted the significance of ML's effect on blockchain security despite their current limitations.

Although ML and blockchain have the potential to revolutionize security, there are still difficulties that should be addressed, such as scalability, interoperability, and privacy concerns, as well as the vulnerability of ML algorithms to adversarial attacks. Federated learning and zero-knowledge proofs are significant advances, and tokenization may be used in conjunction with ML algorithms to identify possible fraud or security risks. Future research should focus on privacy-preserving approaches, improving the efficacy and scalability of ML algorithms, and studying the integration of other cutting-edge technologies with ML and blockchain to build novel and cutting-edge solutions for a wide range of industries and use cases.

Electronic copy available at: https://ssrn.com/abstract=4626844

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Sarker, I.H. Machine learning: Algorithms, real-world applications and research directions. *SN Comput. Sci.* **2021**, *2*, 160. [CrossRef]
2. Taherdoost, H.; Madanchian, M. Artificial Intelligence and Knowledge Management: Impacts, Benefits, and Implementation. *Computers* **2023**, *12*, 72. [CrossRef]
3. De Breuck, P.-P.; Hautier, G.; Rignanese, G.-M. Materials property prediction for limited datasets enabled by feature selection and joint learning with MODNet. *NPJ Comput. Mater.* **2021**, *7*, 83. [CrossRef]
4. Vabalas, A.; Vabalas, A.; Gowen, E.; Poliakoff, E.; Casson, A.J. Machine learning algorithm validation with a limited sample size. *PLoS ONE* **2019**, *14*, e0224365. [CrossRef]
5. Liu, B.; Liu, B.; Ding, M.; Shaham, S.; Rahayu, W.; Farokhi, F.; Lin, Z. When machine learning meets privacy: A survey and outlook. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 31. [CrossRef]
6. Daniel, F.; Daniel, F.; Kucherbaev, P.; Cappiello, C.; Benatallah, B.; Allahbakhsh, M. Quality control in crowdsourcing: A survey of quality attributes, assessment techniques, and assurance actions. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 7. [CrossRef]
7. Jordaney, R.; Jordaney, R.; Sharad, K.; Dash, S.K.; Wang, Z. Transcend: Detecting concept drift in malware classification models. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 16–18 August 2017.
8. Sisinni, E.; Saifullah, A.; Han, S.; Jennehag, U.; Gidlund, M. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4724–4734. [CrossRef]
9. Ye, C.; Li, G.; Cai, H.; Gu, Y.; Fukuda, A. Analysis of security in blockchain: Case study in 51%-attack detecting. In Proceedings of the 2018 5th International Conference on Dependable Systems and Their Applications (DSA), Dalian, China, 22–23 September 2018.
10. Atzei, N.; Bartoletti, M.; Cimoli, T. A survey of attacks on ethereum smart contracts (sok). In Proceedings of the Principles of Security and Trust: 6th International Conference, POST 2017, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2017, Uppsala, Sweden, 22–29 April 2017; Proceedings 6; Springer: Berlin/Heidelberg, Germany, 2017.
11. Buterin, V. A next-generation smart contract and decentralized application platform. *White Pap.* **2014**, *3*, 2-1.
12. Taherdoost, H. Smart Contracts in Blockchain Technology: A Critical Review. *Information* **2023**, *14*, 117. [CrossRef]
13. Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1153–1176. [CrossRef]
14. Usman, M.; Jan, M.A.; He, X.; Chen, J. A survey on representation learning efforts in cybersecurity domain. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 111. [CrossRef]
15. Mahdavifar, S.; Ghorbani, A.A. Application of deep learning to cybersecurity: A survey. *Neurocomputing* **2019**, *347*, 149–176. [CrossRef]
16. Kumble, G.P. *Practical Artificial Intelligence and Blockchain: A Guide to Converging Blockchain and AI to Build Smart Applications for New Economies*; Packt Publishing Ltd.: Birmingham, UK, 2020.
17. Habib, G.; Sharma, S.; Ibrahim, S.; Ahmad, I.; Qureshi, S.; Ishfaq, M. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet* **2022**, *14*, 341. [CrossRef]
18. Craig, W.L.; Park, W.W.; Paulsson, J. *International Chamber of Commerce Arbitration*; Oceana Publications: New York, NY, USA, 1990; Volume 3.
19. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
20. Cai, C.W. Disruption of financial intermediation by FinTech: A review on crowdfunding and blockchain. *Account. Financ.* **2018**, *58*, 965–992. [CrossRef]
21. Stephen, R.; Alex, A. Alex, A. A review on blockchain security. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2018.
22. Hong, H.; Sun, Z. A secure peer to peer multiparty transaction scheme based on blockchain. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 1106–1117. [CrossRef]
23. Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*; John Wiley & Sons: Hoboken, NJ, USA, 2020.
24. Xinyi, Y.; Yi, Z.; He, Y. Technical characteristics and model of blockchain. In Proceedings of the 2018 10th international Conference on Communication Software and Networks (ICCSN), Chengdu, China, 6–9 July 2018.
25. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [CrossRef]
26. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2794–2830. [CrossRef]
27. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain meets cloud computing: A survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2009–2030. [CrossRef]

Electronic copy available at: https://ssrn.com/abstract=4626844

28. Wang, W.; Huang, H.; Zhang, L.; Su, C. Secure and efficient mutual authentication protocol for smart grid under blockchain. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 2681–2693. [CrossRef]
29. Wang, W.; Huang, H.; Zhang, L.; Han, Z.; Qiu, C.; Su, C. BlockSLAP: Blockchain-based secure and lightweight authentication protocol for smart grid. In Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 January 2021.
30. Taherdoost, H. A critical review of blockchain acceptance models—Blockchain technology adoption frameworks and applications. *Computers* **2022**, *11*, 24. [CrossRef]
31. Kulkarni, N.; Pise, R.; Patil, S. *A Deep Dive into Blockchain Consensus Algorithms, in Blockchain for Smart Systems*; Chapman and Hall/CRC: Boca Raton, FL, USA, 2022; pp. 67–82.
32. Sayadi, S.; Rejeb, S.B.; Choukair, Z. Blockchain challenges and security schemes: A survey. In Proceedings of the 2018 Seventh International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, 1–3 November 2018.
33. Göbel, J.; Keeler, H.P.; Krzesinski, A.E.; Taylor, P.G. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Perform. Eval.* **2016**, *104*, 23–41. [CrossRef]
34. Tosh, D.K.; Shetty, S.; Liang, X.; Kamhoua, C.A.; Kwiat, K.A.; Njilla, L. Security implications of blockchain cloud with analysis of block withholding attack. In Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, Spain, 14–17 May 2017.
35. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Proceedings of the Advances in Cryptology—CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; Proceedings, Part I.. Springer: Berlin/Heidelberg, Germany, 2017.
36. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A survey on blockchain technology: Evolution, architecture and security. *IEEE Access* **2021**, *9*, 61048–61073. [CrossRef]
37. Singh, S.; Hosen, A.S.; Yoon, B. Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access* **2021**, *9*, 13938–13959. [CrossRef]
38. Taherdoost, H. Blockchain Technology and Artificial Intelligence Together: A Critical Review on Applications. *Appl. Sci.* **2022**, *12*, 12948. [CrossRef]
39. Mayo, M. Frameworks for approaching the machine learning process. *KDnuggets*, 19 October 2018.
40. Balusamy, B.; Chilamkurti, N.; Beena, L.A.; Poongodi, T. Blockchain and Machine Learning for e-Healthcare Systems. The Institution of Engineering and Technology. 2021. Available online: https://www.amazon.ca/Blockchain-Machine-Learning-Healthcare-Systems/dp/1839531142 (accessed on 1 May 2023).
41. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N. Verification and validation techniques for streaming big data analytics in internet of things environment. *IET Netw.* **2019**, *8*, 155–163. [CrossRef]
42. Gaur, R.; Prakash, S.; Kumar, S.; Abhishek, K.; Msahli, M.; Wahid, A. A Machine-Learning–Blockchain-Based Authentication Using Smart Contracts for an IoHT System. *Sensors* **2022**, *22*, 9074. [CrossRef]
43. Mrabet, H.; Alhomoud, A.; Jemai, A.; Trentesaux, D. A Secured Industrial Internet-of-Things Architecture Based on Blockchain Technology and Machine Learning for Sensor Access Control Systems in Smart Manufacturing. *Appl. Sci.* **2022**, *12*, 4641. [CrossRef]
44. Hamodi, Y.I.; Aljanabi, Y.I.; Majeed, A.A.; Jihad, K.H.; Qader, B.A. Detect and Mitigate Blockchain-Based DDoS Attacks Using Machine Learning and Smart Contracts. *Informatica* **2022**, *46*, 55–62.
45. Shahbazi, Z.; Byun, Y.C. Blockchain-Based Event Detection and Trust Verification Using Natural Language Processing and Machine Learning. *IEEE Access* **2022**, *10*, 5790–5800.
46. Zhou, Q.; Zheng, K.; Zhang, K.; Hou, L.; Wang, X. Vulnerability Analysis of Smart Contract for Blockchain-Based IoT Applications: A Machine Learning Approach. *IEEE Internet Things J.* **2022**, *9*, 24695–24707. [CrossRef]
47. Al-Qarafi, A.; Alrowais, F.; Alotaibi, S.S.; Nemri, N.; Al-Wesabi, F.N.; Al Duhayyim, M.; Marzouk, R.; Othman, M.; Al-Shabi, M. Optimal Machine Learning Based Privacy Preserving Blockchain Assisted Internet of Things with Smart Cities Environment. *Appl. Sci.* **2022**, *12*, 5893. [CrossRef]
48. Tian, Y.; Tian, Y.; Li, T.; Xiong, J.; Bhuiyan, M.Z.A.; Ma, J.; Peng, C. A Blockchain-Based Machine Learning Framework for Edge Services in IIoT. *IEEE Trans. Ind. Inform.* **2022**, *18*, 1918–1929. [CrossRef]
49. Yu, Y.; Chen, R.; Li, H.; Li, Y.; Tian, A. Toward data security in edge intelligent IIoT. *IEEE Netw.* **2019**, *33*, 20–26. [CrossRef]
50. Liu, X.; Xie, L.; Wang, Y.; Zou, J.; Xiong, J.; Ying, Z.; Vasilakos, A.V. Privacy and security issues in deep learning: A survey. *IEEE Access* **2020**, *9*, 4566–4593. [CrossRef]
51. Hasan, N.; Chaudhary, K.; Alam, M. A novel blockchain federated safety-as-a-service scheme for industrial IoT using machine learning. *Multimed. Tools Appl.* **2022**, *81*, 36751–36780. [CrossRef]
52. Aldughayfiq, B.; Sampalli, S. Patients', pharmacists', and prescribers' attitude toward using blockchain and machine learning in a proposed ePrescription system: Online survey. *JAMIA Open* **2022**, *5*, ooab115. [CrossRef]
53. Kumar, P.; Kumar, R.; Srivastava, G.; Gupta, G.P.; Tripathi, R.; Gadekallu, T.R.; Xiong, N.N. PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2326–2341. [CrossRef]
54. Khan, M.A.; Khan, M.A.; Abbas, S.; Rehman, A.; Saeed, Y.; Zeb, A.; Uddin, M.I.; Nasser, N.; Ali, A. A Machine Learning Approach for Blockchain-Based Smart Home Networks Security. *IEEE Netw.* **2021**, *35*, 223–229. [CrossRef]

Electronic copy available at: https://ssrn.com/abstract=4626844

55. Yi, H. Securing instant messaging based on blockchain with machine learning. *Saf. Sci.* **2019**, *120*, 6–13. [CrossRef]
56. Zhang, R.; Song, M.; Li, T.; Yu, Z.; Dai, Y.; Liu, X.; Wang, G. Democratic learning: Hardware/software co-design for lightweight blockchain-secured on-device machine learning. *J. Syst. Archit.* **2021**, *118*, 102205. [CrossRef]
57. Benjamin Franklin, I.; Jerald, M.P.A.; Bhuvaneswari, R. Machine Learning-Based Trust Management in Cloud Using Blockchain Technology. *SN Comput. Sci.* **2022**, *3*, 429. [CrossRef]
58. Priyadharshini, K.; Canessane, R.A. Light chain consensus reinforcement machine learning: An effective blockchain model for Internet of Things using for its advancement and challenges. *Comput. Intell.* **2021**, *37*, 1651–1672. [CrossRef]
59. Vairagade, R.S.; Brahmananda, S.H. Enabling machine learning-based side-chaining for improving QoS in blockchain-powered IoT networks. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4433. [CrossRef]
60. Vargas, H.; Lozano-Garzon, C.; Montoya, G.A.; Donoso, Y. Detection of security attacks in industrial IoT networks: A blockchain and machine learning approach. *Electronics* **2021**, *10*, 2662. [CrossRef]
61. Choudhary, S.; Dorle, S. A quality of service-aware high-security architecture design for software-defined network powered vehicular ad-hoc networks using machine learning-based blockchain routing. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6993. [CrossRef]
62. Pon, P.; Kavitha, V. Blockchain based cloud service security architecture with distributed machine learning for smart device traffic record transaction. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e683. [CrossRef]
63. Nasir, M.U.; Nasir, M.U.; Khan, S.; Mehmood, S.; Khan, M.A.; Zubair, M.; Hwang, S.O. Network Meddling Detection Using Machine Learning Empowered with Blockchain Technology. *Sensors* **2022**, *22*, 6755. [CrossRef]
64. Unal, D.; Hammoudeh, M.; Khan, M.A.; Abuarqoub, A.; Epiphaniou, G.; Hamila, R. Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. *Comput. Secur.* **2021**, *109*, 102393. [CrossRef]
65. Shahin, R.; Sabri, K.E. A Secure IoT Framework Based on Blockchain and Machine Learning. *Int. J. Comput. Digit. Syst.* **2022**, *11*, 671–683. [CrossRef]
66. Jamil, F.; Kahng, H.K.; Kim, S.; Kim, D.H. Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms. *Sensors* **2021**, *21*, 1640. [CrossRef] [PubMed]
67. Kim, H.; Kim, S.H.; Hwang, J.Y.; Seo, C. Efficient privacy-preserving machine learning for blockchain network. *IEEE Access* **2019**, *7*, 136481–136495. [CrossRef]
68. Shahbazi, Z.; Byun, Y.C. Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing. *Sensors* **2021**, *21*, 1467. [CrossRef] [PubMed]
69. Shahbazi, Z.; Byun, Y.C. Blockchain and machine learning for intelligent multiple factor-based ride-hailing services. *Comput. Mater. Contin.* **2022**, *70*, 4429–4446. [CrossRef]
70. Kumar, P.; Gupta, G.P.; Tripathi, R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *J. Syst. Archit.* **2021**, *115*, 101954. [CrossRef]
71. Agrawal, S.; Kumar, S. MLSMBQS: Design of a Machine Learning Based Split & Merge Blockchain Model for QoS-Aware Secure IoT Deployments. *Int. J. Image Graph. Signal Process.* **2022**, *14*, 58–71. [CrossRef]
72. Wang, H.; Wang, Y.; Cao, Z.; Li, Z.; Xiong, G. An overview of blockchain security analysis. In Proceedings of the Cyber Security: 15th International Annual Conference, CNCERT 2018, Beijing, China, 14–16 August 2018; Revised Selected Papers 15. Springer: Singapore, 2019.
73. Du, R.; Gao, Y.; Liu, C. Fine-grained Web Service Trust Detection: A Joint Method of Machine Learning and Blockchain. *J. Web Eng.* **2022**, *21*, 1519–1542. [CrossRef]
74. Ashfaq, T.; Ashfaq, T.; Khalid, M.I.; Ali, G.; Affendi, M.E.; Iqbal, J.; Hussain, S.; Ullah, S.S.; Yahaya, A.S.; Khalid, R.; et al. An Efficient and Secure Energy Trading Approach with Machine Learning Technique and Consortium Blockchain. *Sensors* **2022**, *22*, 7263. [CrossRef]
75. Ashfaq, T.; Khalid, R.; Yahaya, A.S.; Aslam, S.; Azar, A.T.; Alsafari, S.; Hameed, I.A. A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors* **2022**, *22*, 7162. [CrossRef]
76. Sajid, M.B.E.; Ullah, S.; Javaid, N.; Ullah, I.; Qamar, A.M.; Zaman, F. Exploiting Machine Learning to Detect Malicious Nodes in Intelligent Sensor-Based Systems Using Blockchain. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 7386049. [CrossRef]
77. Xiong, W.; Xiong, L. Smart Contract Based Data Trading Mode Using Blockchain and Machine Learning. *IEEE Access* **2019**, *7*, 102331–102344. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Electronic copy available at: https://ssrn.com/abstract=4626844